

Roadmap DIN 27002/27009 („KRITIS“)

Gefahrenlage in der Praxis

Rainer Bachmann, enerson consulting

Köln, 16. Juli 2013

▶ • **Management Zusammenfassung**

- KRITIS Szenarien: Fall 1
- KRITIS Szenarien: Fall 2
- Videos
- Links

MANAGEMENT ZUSAMMENFASSUNG

Grund- lage

**Nationale Strategie zum Schutz Kritischer Infrastrukturen
(KRITIS-Strategie)**
Grundlagenpapier des Bundesministerium des Innern aus 2009

Umsetzung

Technische Basisinfrastrukturen

- Energieversorgung
- Informations- und Kommunikationstechnologie
- Transport und Verkehr
- (Trink-) Wasserversorgung und Abwasserentsorgung

Sozioökonomische Dienstleistungs-Infrastrukturen

- Gesundheitswesen, Ernährung
- Notfall- und Rettungswesen, Katastrophenschutz
- Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen
- Finanz- und Versicherungswesen
- Medien und Kulturgüter

Ergänzende Dokumente

Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung
Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, November 2010

Die Bundesregierung formuliert eine Nationale Strategie zum Schutz Kritischer Infrastrukturen – die Industrie ist dringend zur Umsetzung aufgefordert.

MANAGEMENT ZUSAMMENFASSUNG

**Grund-
lage**

**Nationale Strategie zum Schutz Kritischer Infrastrukturen
(KRITIS-Strategie)**
Grundlagenpapier des Bundesministerium des Innern aus 2009

Umsetzung

**Technische
Basisinfrastrukturen**

- Energieversorgung
- Informations- und Kommunikationstechnologie
- Transport und Verkehr
- (Trink-) Wasserversorgung und Abwasserentsorgung

**Sozioökonomische
Dienstleistungs-Infrastrukturen**

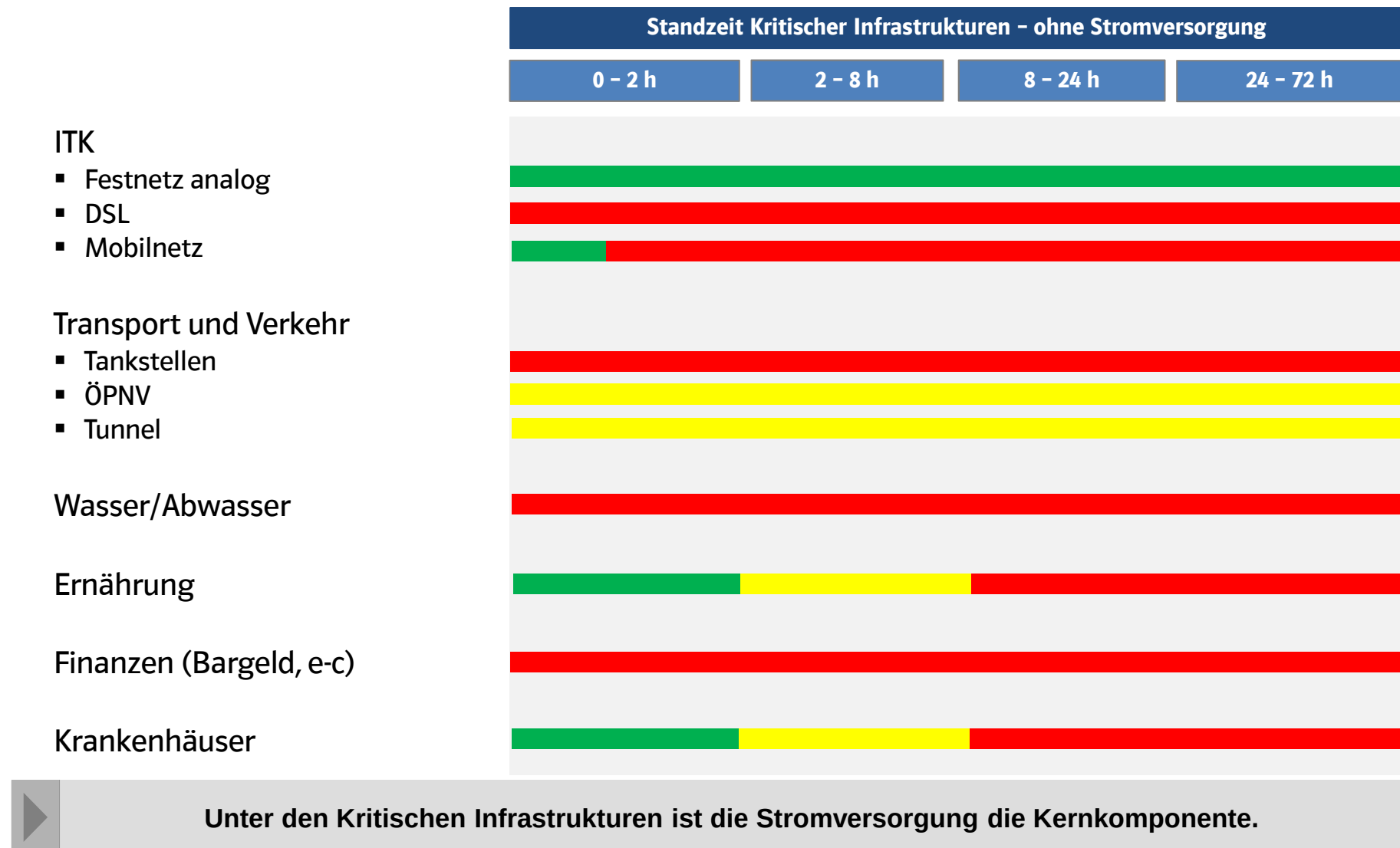
- Gesundheitswesen, Ernährung
- Notfall- und Rettungswesen, Katastrophenschutz
- Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen
- Finanz- und Versicherungswesen
- Medien und Kulturgüter

**Ergänzende
Dokumente**

Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen Ausfalls der Stromversorgung; Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, November 2010

Unter den Kritischen Infrastrukturen hat die Energieversorgung und dort die Stromversorgung die höchste Kritikalität.

MANAGEMENT ZUSAMMENFASSUNG



- Management Zusammenfassung
 - ▶ • **KRITIS Szenarien: Fall 1**
-
- KRITIS Szenarien: Fall 2
 - Videos
 - Links

KRITIS SZENARIEN

- **Szenario 1- Angriff auf Umspannstationen**
 - Schadensfall und Auswirkungen
 - Ursache
 - Fehleranalyse und -behebung
 - Beschleunigung der Analyse und Behebung
 - Prävention

SZENARIO 1: ANGRIFF AUF UMSPANNSTATIONEN

SCHADENSFALL UND AUSWIRKUNGEN

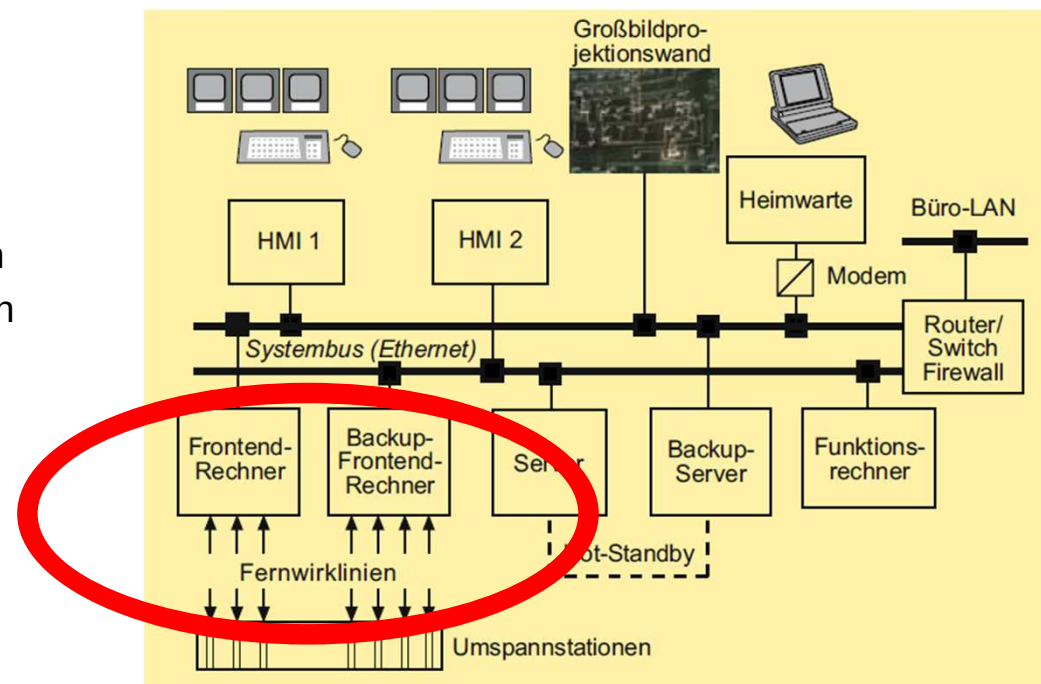
- Ausfall einer großen Anzahl (10 - 100) von steuerbaren Umspannstationen (MS $\leftrightarrow$ NS) bzw. MS-Schaltanlagen
- Großflächiger Ausfall der Stromversorgung (n-1-Prinzip „ausgehebelt“)
- Zugriff auf Umspannstationen und Fernwirkung unmöglich
- Eventuell Neuparametrierung und manueller Wiederanlauf der Stationen erforderlich
- Vollständiger Wiederanlauf nach 3 Tagen (siehe Ablaufprotokoll)



SZENARIO 1: ANGRIFF AUF UMSPANNSTATIONEN

URSACHE

- Schadsoftware über Wartungsschnittstelle vor Ort eingeschleust
- Umspannstation kommuniziert in Echtzeit mit den Frontend-Rechnern in der Netzleitstelle
- Schadsoftware verbreitet sich über diese zentrale Schnittstelle unbemerkt auf alle verbundenen Umspannstationen
- Schadsoftware wird zu einem bestimmten Zeitpunkt aktiv und stört dann die Kommunikation mit den Frontend-Rechnern
- Schaltverhalten der Umspannstationen kann nicht mehr gesteuert werden
- Schadsoftware deaktiviert niederspannungsseitig alle befallenen Umspannstationen



SZENARIO 1: ANGRIFF AUF UMSPANNSTATIONEN

FEHLERANALYSE/-BEHEBUNG

Fehler- analyse

- **Vor-Ort-Analyse: System lässt sich neu starten aber nicht mehr fernsteuern**
- **Kontaktaufnahme mit der internen IT (1. LS)**
- **Kontaktaufnahme mit SCADA-Hersteller (2. LS)**
- **Fernanalyse NLS ergibt keinen Fehler**
- **Fernanalyse USpSt nicht möglich, daher Software-Fehlerdiagnose durch den Hersteller vor Ort**
- **Fehleridentifikation**

Fehler- behebung

- **Meldung an die Meldestelle**
- **Herstellung einer lauffähigen Version mit Original-SCADA-Software**
- **Test der Kommunikation an einer einzelnen Umspannstation im Zusammenspiel mit Netzleitstelle**
- **Übernahme der Parametrierung**
- **Unterbindung des erneuten Transfers des Virus**
- ◆ **Systemwiederherstellung erfolgreich**
- **Bereitstellung mehrerer Programmierstationen**
- **Ausrollen der Lösung auf Umspannstationen durch Netzservicetechniker - vor Ort**
- **Priorisierung im Wiederanlauf**
 - Prio A: KRITIS-Einrichtungen
 - Prio B: Städte? Landwirtschaft? Nicht-notstromversorgte relevante Einrichtungen?
 - Prio C: ..
- ◆ **Wiederanlauf komplett**

SZENARIO 1: ANGRIFF AUF UMSPANNSTATIONEN

BESCHLEUNIGUNG DER FEHLERANALYSE/-BEHEBUNG

Analyse

- Zutrittsprotokolle
- Zugriffsprotokolle
- Integritätsprüfung der dezentralen SCADA-Komponenten

Vorbereitung

- Aktuelle Kontaktdaten aller Hersteller, DL, Lieferanten und KRITIS Kunden
- Zugriff auf externe Ressourcen z.B. beim Rollout der neuen Software
- Konfigurationsparameter dezentraler Systemkomponenten zentral und gesichert speichern (durch Verschlüsselung)
- 2-3 Versionen lauffähiger Anwendungen vorhalten
- ...

Behebung

- Programmiergeräte ausrüsten
- Lauffähige Version bereitstellen
- Konfigurationsparameter dezentraler Systemkomponenten einspielen
- Informationen über Energiebedarfe von KRITIS-Einrichtungen und vorhandene Notstrom-Versorgung bzw. dezentrale Erzeugung
- Roll-Out planen
- Netzbetrieb wiederaufnehmen

Bei einem Netzausfall entwickelt sich die wirtschaftliche Höhe des Schadens exponentiell in Bezug auf die Ausfalldauer.

SZENARIO 1: ANGRIFF AUF UMSPANNSTATIONEN

PRÄVENTION

generell

- Bei „Vandalismus“/Manipulationsverdacht: Routineüberprüfung auch der Software
- Schnittstelle verschlüsseln oder Schnittstelle manipulationssicher gestalten
- Fernwirklinien redundant auslegen
- Frontend-Rechner redundant auslegen
- Frontend-Rechner durch entsprechende Firewalls und Antiviren-Programme schützen
- Regelmäßige war-games durchspielen, dadurch 95% der Lücken schließen (bezogen auf Cyber-Attacks)

Zugriff, Zugang und Zutritt

Umspannstation

- Baulich den Zutritt erschweren
- Zugang sicherer gestalten z.B. durch Einsatz von Alarmsicherung der Türen, Kameraüberwachung etc.
- Zugangs- und Zugriffsprotokolle kontrollieren
- Ergänzende Sicherungsverfahren ...

Personal

- Eigenes Personal: regelmäßige Sicherheitsüberprüfung
- Fremd-Dienstleister: Vereinbarung über regelmäßige Sicherheitsüberprüfung
- System-Lieferanten: Erklärung zur regelmäßigen Sicherheitsüberprüfung

- Management Zusammenfassung
 - KRITIS Szenarien: Fall 1
 - ▶ • **KRITIS Szenarien: Fall 2**
-
- Videos
 - Links

- **Szenario 2- Angriff auf Netzleitstelle**
 - Schadensfall und Auswirkungen
 - Ursache
 - Fehleranalyse und -behebung
 - Beschleunigung der Analyse und Behebung
 - Prävention

SZENARIO 2: ANGRIFF AUF NETZLEITSTELLE

SCHADENSFALL UND AUSWIRKUNG

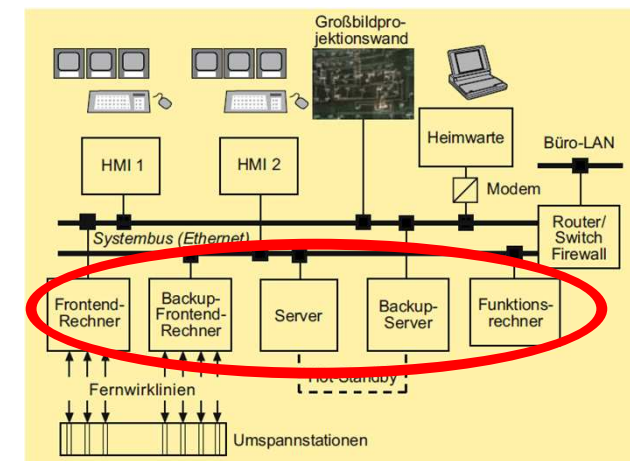
- Lastflussdaten in der Netzleitstelle sind manipuliert
 - Netzleitung trifft fehlerhafte Entscheidungen: Überspannungen im Netzgebiet
 - Automatische Routinen wie Lastabwurf oder Wiederanlauf werden wiederholt fehlerhaft ausgelöst bzw. gestartet
 - Hot-Standby-System ebenfalls infiziert: kein geregelter Betrieb möglich
-
- Infrastrukturschäden durch Überspannung oder Überfrequenz
 - Komplette Netzabschaltung



SZENARIO 2: ANGRIFF AUF NETZLEITSTELLE

URSACHE

- Fernwartungssystem des Herstellers der Netzleitstellenrechnersoftware wurde physikalisch manipuliert (mobiles Gerät zwischengeschaltet)
- Bei nächstem Fernwartungsvorgang wird der Zugang durch die Netzleitstelle freigegeben
- Mobiles Fremdgerät registriert die Aktivität der digitalen Wartungslinien, fängt den Datenverkehr des nächsten Updates ab und verändert die Datenpakete
- Schadsoftware platziert sich im Grundbetriebssystem (z.B. Bios)
- Schadsoftware verfälscht Daten des Lastmanagements und des Bezugsmanagements



SZENARIO 2: ANGRIFF AUF NETZLEITSTELLE

FEHLERANALYSE/-BEHEBUNG

Fehler- analyse

- Kontaktaufnahme mit der
 - internen IT (1. LS)
 - IT und/oder TK-Dienstleister
 - SCADA-Hersteller (2. LS)
- Überprüfung der Schaltanlagen durch Betriebsdienst im ausgewählten Inselnetz
- Ausschluss von Defekten an der physikalischen Infrastruktur
- Fehleridentifikation durch IT (eventuell nach Vergleich der Messdaten zwischen Leitstelle und Feld-/Stationsrechner)

Fehler- behebung

- ...
- ♦ • Neukonfiguration des gesamten Betriebssystems
- Steuersoftware wird installiert
- ...
- ♦ • Wiederanlauf der Leitstelle und des Netzes starten

SZENARIO 2: ANGRIFF AUF NETZLEITSTELLE

BESCHLEUNIGUNG DER FEHLERANALYSE/-BEHEBUNG

Analyse

- Zugriffsprotokollen (log-files)
- Testverfahren (ping)
- Funktionsprüfung / Simulation
- Integritätsprüfung

Vorbereitung

- ...
- Notfallkonzeption im Vorfeld erstellen und testen
- Verfahren müssen regelmäßig, insbesondere nach System-Updates getestet werden
- Dokumentierte Verfahren zur Datensicherung/-wiederherstellung
- Rollback-Funktion auf festgelegte Anzahl von Konfigurationszuständen

Behebung

- Back-up einsetzen
- Ersatzsysteme einsetzen
- Systemdateien und –updates von ROMs lesen und einsetzen
- ...
- Informationen über Energiebedarfe von KRITIS-Einrichtungen und vorhandene Notstrom-Versorgung bzw. dezentrale Erzeugung
- Roll-Out planen
- Netzbetrieb wiederaufnehmen

Bei einem Netzausfall entwickelt sich die wirtschaftliche Höhe des Schadens exponentiell in Bezug auf die Ausfalldauer.

SZENARIO 2: ANGRIFF AUF NETZLEITSTELLE

PRÄVENTION

System- Entwicklung und Wartung

- Testverfahren, z.B. Laufzeitmessung der Signale als Hinweis auf ein zwischengeschaltetes Gerät geben (Stichwort: Ping, Round-Trip time)
- Systemupdates immer zuerst auf isoliertem Testsystem anwenden und protokollieren
- mehrere Generationen lauffähiger Releases des Gesamtsystem bezogen auf die kritischen Komponenten und Anwendungen vorhalten
- umfangreiche Release-Tests und Integritätskontroll-Mechanismen
- Lieferanten bewusst wählen >> Einkaufsprozess
- ...

Zugriff, Zugang und Zutritt

- Zugang und Zugriff mindestens durch eine starke 2-Faktor-Authentifizierung (z.B. Verbindung von Zugangskarten und Codenummern) sichern und protokollieren
- Systemwartung über Fernwartungszugang soweit wie möglich einschränken
- Fernwartung beobachten
- Fremd-Dienstleister: Vereinbarung über regelmäßige Sicherheitsüberprüfung
- System-Lieferanten: Erklärung zur regelmäßigen Sicherheitsüberprüfung
- ...

- Management Zusammenfassung
- KRITIS Szenarien: Fall 1
- KRITIS Szenarien: Fall 2

▶ • **Videos**

-
- Links

- Management Zusammenfassung
- KRITIS Szenarien: Fall 1
- KRITIS Szenarien: Fall 2
- Videos

▶ • **Links**

LINKS

Blackout in Österreichs Stromnetzen

- <http://fm4.orf.at/stories/1717900/>

München: Kurzschluss löste Stromausfall aus

- <http://www.sueddeutsche.de/muenchen/blackout-in-muenchen-kurzschluss-loeste-stromausfall-aus-1.1549424>

Angriff auf 50Hertz

- <http://www.welt.de/wirtschaft/energie/article111369975/Russische-Hacker-attackieren-Stromnetzbetreiber.html>

Aurora-Projekt:

Video: www.youtube.com/watch?v=fJyWngDco3g

Verifizierung des Videos anhand folgender Quellen:

- CNN Artikel: edition.cnn.com/2007/US/09/26/power.at.risk/index.html?_s=PM:US
- Department of Homeland Security: www.oig.dhs.gov/assets/Mgmt/OIG_09-95_Aug09.pdf

Arte Dokumentation „Cyber war“:

- Link zu Estland: www.youtube.com/watch?v=jcusSytrD4A (zwischen 02:39 min und 07:20 min)
- Link zu Cyberangriff auf Versorgungsnetze: www.youtube.com/watch?v=Y41CbmedHf8 (zwischen 06:25 min und 10:40 min)

Spiegel-Bericht zu Stuxnet (Spiegel 16/2011):

- www.spiegel.de/spiegel/print/d-78076193.html

TAB-Arbeitsbericht Nr. 141 (Berlin 2010):

- www.tab-beim-bundestag.de/de/publikationen/berichte/ab141.html

- ▶ • **danke für Ihre Aufmerksamkeit ...**
-